CSC2125 Homework 5

Zi Han Zhao

1001103708

1 What would happen if a powerful attacker identifies all participants of one shard in OmniLedger and launches DDoS attacks to take down the participants of the shard (make them offline)? Will this attack affect transactions in other shards?

OmniLedger introduces a new consensus protocol: ByzCoinX, which is the improved version of PBFT-based ByzCoin. First, ByzCoinX parallelizes block commitments. It is capable of identifying the non-conflict transactions and processing the transactions safely. If DDoS attack shuts down one whole shard chain, all of other non-conflict transactions can still be processed in other shards. They are not affected. Second, cross-shard transactions follow Atomix protocol. If one shard fails, the abortion of the transaction is triggered in order to avoid the kind of transaction being processed by other shards. Third, OmniLedger's group-communication pattern has a high probability of convergence under faults. If a shard halts under DDoS attack, a new shard is created and a new shard leader will be elected with 97% probability of successfully reaching consensus. Other shards still work as normal.

2 What would happen if the attacker is able to even bribe the participants to process invalid transactions? Will this attack affect transactions in other shards?

Validators exist in each shard. They will validate and process all of the transactions on the chain. The invalid transaction will be reverted on the shard chain. Also, if the attacker brides validator to be a malicious one. During each epoch round, the validators will be assigned randomly into different shards. Also a near-fixed ratio of honest and malicious validators are assumed in threat model in the paper. It is proved that under such ratio, it is impossible to process a invalid transaction successfully.

3 Is Monoxide running 64 parallel Nakamoto consensus chains (without Chukonu mining) less secure than the original Bitcoin consensus? Why?

Yes. Without Chukonu mining, miner power dilution occurs in 64 chains. Independent growth of per-zone chain causes mining power distributed across zones. Then each zone receives 1/n mining power of the entire network. It results in a much lowered attack bar, even lower than 1%. So it is called 1% attack. It is less secure than original Bitcoin network.

4 Suppose a Monoxide node is using Chukonu mining on k shards. How many resources (e.g., storage, computation, etc.) the node would need comparing to a node without Chukonu mining? Is sharding really useful in this Chukonu mining case?

If miners participate mining for m zones out of k, the resource is roughly m times larger than without Chukonu mining. Because the miner will calculate block header for m block headers from m consecutive zones. Besides, more IT resources are needed to sync the zones and validate blocks in order to participate mining.

Is sharding really useful in this Chukonu mining case?

My answer is yes or no.

Chukonu mining aims to solve the attack with much lower computation power. The attack appears under the sharding blockchain network. We can say that such sharding networks is the reason why using Chukonu mining. Also, in Chukonu mining, it is incentive for miners to participate more zones (i.e. more shards) to earn more rewards. So sharding is useful in such network.

However, sharding makes the Chukonu miners need more computation resources (storage) to store additional structure for different zones. The consumption will increase. So it is not helpful.